



Troubleshooting Guide for Cisco Unified MeetingPlace Express Release 1.2

Includes Cisco Unified MeetingPlace Express VT Release 1.2

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-11303-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This Software includes software governed by certain open source licenses as follows:

LAME 3.xx found at <http://www.mp3dev.org>.
LAME Ain't an MP3 Encoder
<http://www.mp3dev.org>
March 2001

Originally developed by Mike Cheng (www.uq.net.au/~zzmcheng).
Now maintained by Mark Taylor (www.mp3dev.org).

This code is distributed under the GNU LESSER PUBLIC LICENSE (LGPL, see www.gnu.org) with the following modification:

If you determine that distribution of LAME requires a patent license, and you obtain a patent license, you may distribute LAME even though redistribution of LAME may also require a patent license.

You agree not to enforce any patent claims for any aspect of MPEG audio compression, or any other techniques contained in the LAME source code.

LAME uses the MPGLIB decoding engine, from the MPG123 package, written by: Michael Hipp (www.mpg123.de) MPGLIB is released under the GPL.

Copyrights (c) 1999,2000,2001 by Mark Taylor
Copyrights (c) 1998 by Michael Cheng
Copyrights (c) 1995,1996,1997 by Michael Hipp: mpplib

As well as additional copyrights as documented in the source code.

If you cannot locate copies of the referenced GPL license(s) in this section please contact the Free Software Foundation at licensing@fsf.org or 51 Franklin St., 5th Floor, Boston, MA 02110-1301. For information about obtaining the source code for the third party software, contact Cisco Systems Legal Department and include details about the product and a copy of the license at 300 E. Tasman Dr., San Jose, CA 95124.

Portions of this software product are copyright as follows:

Copyright (c) 1985, 1987, 1988 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software product include the following notice:

This file is in the public domain, so clarified as of 1996-06-05 by Arthur David Olson (arthur_david_olson@nih.gov)

Adobe technology is used in this product.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study,

LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Troubleshooting Guide for Cisco Unified MeetingPlace Express Release 1.2
Copyright © 2005-2006 Cisco Systems, Inc. All rights reserved.



Preface	i
Purpose	i
Audience	i
Organization	ii
Related Documentation	ii
Conventions	iii
Obtaining Documentation	iii
Cisco.com	iii
Product Documentation DVD	iv
Ordering Documentation	iv
Documentation Feedback	iv
Cisco Product Security Overview	iv
Reporting Security Problems in Cisco Products	v
Product Alerts and Field Notices	v
Obtaining Technical Assistance	vi
Cisco Technical Support & Documentation Website	vi
Submitting a Service Request	vii
Definitions of Service Request Severity	vii
Obtaining Additional Publications and Information	vii

CHAPTER 1**Troubleshooting Access Issues for the Cisco Unified MeetingPlace Express System 1-1**

Recovering the Password for the root User Account	1-1
Recovering the Password for the mpadmin Account	1-2
Recovering the System Administrator Password Used in the End-User Interface and the Administration Console	1-3
Accessing the System after Uploading the Wrong SSL Certificate or Key	1-4
Troubleshooting a Failed LDAP Log On Attempt	1-5

CHAPTER 2**Backing Up, Archiving, and Restoring Data in Cisco Unified MeetingPlace Express 2-1**

Backing Up Data	2-1
Archiving Data	2-2
Restoring Data	2-2

CHAPTER 3

Common Telephone Issues in Cisco Unified MeetingPlace Express 3-1

- Tips for Failed Calls 3-1
- Undetected Key Presses 3-2
- Failed Incoming Calls 3-3
- Dropped Calls 3-3
- Dead Air During Calls 3-4
- Dropped Packets 3-4
- Unable to Call Out 3-5

CHAPTER 4

Exception Codes and Module Numbers Used in Cisco Unified MeetingPlace Express 4-1

- Exception Codes 4-1
- Module Numbers 4-7

CHAPTER 5

General Troubleshooting Tips for the Cisco Unified MeetingPlace Express System 9

- Swapping Out a Disk Drive 9
 - Swapping Out a Disk Drive on a Cisco MCS 7825 10
 - Swapping Out a Disk Drive on a Cisco MCS 7835 or Cisco MCS 7845 10
- File Locations 10
- Troubleshooting a Licensing Error Problem 11
- Troubleshooting a Problem with Excessive Random E-Mails Being Sent 11
- Troubleshooting a Problem with the Web Page Not Coming Up 12

INDEX



Preface

This preface contains the following sections:

- [Purpose, page i](#)
- [Audience, page i](#)
- [Organization, page ii](#)
- [Related Documentation, page ii](#)
- [Conventions, page iii](#)
- [Obtaining Documentation, page iii](#)
- [Documentation Feedback, page iv](#)
- [Cisco Product Security Overview, page iv](#)
- [Product Alerts and Field Notices, page v](#)
- [Obtaining Technical Assistance, page vi](#)
- [Obtaining Additional Publications and Information, page vii](#)

Purpose

The *Troubleshooting Guide for Cisco Unified MeetingPlace Express Release 1.2* provides the information you need to troubleshoot problems in the Cisco Unified MeetingPlace Express system.



Note

This document only covers how to troubleshoot problems that do not occur in the Administration Center or End-User Interface. For information about troubleshooting problems that occur in the Administration Center or End-User Interface, see the [“Related Documentation” section on page ii](#).

This guide does not describe how to install or upgrade your Cisco Unified MeetingPlace Express system, perform system administrator tasks in the Administration Center, or use the End-User Interface.

Audience

This guide is intended for system administrators only. It is not intended for end users.

Organization

This guide contains the following chapter:

- Chapter 1, “Troubleshooting Access Issues for the Cisco Unified MeetingPlace Express System”
- Chapter 2, “Backing Up, Archiving, and Restoring Data in Cisco Unified MeetingPlace Express”
- Chapter 3, “Common Telephone Issues in Cisco Unified MeetingPlace Express”
- Chapter 4, “Exception Codes and Module Numbers Used in Cisco Unified MeetingPlace Express”
- Chapter 5, “General Troubleshooting Tips for the Cisco Unified MeetingPlace Express System”

Related Documentation

General Information

For complete information about all of the Cisco conferencing documentation, see the *Guide to Cisco Unified Conferencing Documentation and Support* at the following URL:

http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html

Installation and Upgrade

Information about installing and upgrading Cisco Unified MeetingPlace Express can be found in the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2* at the following URL:

http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html

Configuration and Maintenance

If you want information about configuring and maintaining your Cisco Unified MeetingPlace Express system or about troubleshooting problems in the Administration Center, see one of the following:

- *Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2* at the following URL:
http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html
- Online help found in the Cisco Unified MeetingPlace Express Administration Center

End User Help

If you want information about using or troubleshooting the End-User Interface portion of the Cisco Unified MeetingPlace Express system see one of the following:

- *User Guide for Cisco Unified MeetingPlace Express Release 1.2* at the following URL:
http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html
- Online help found in the Cisco Unified MeetingPlace Express End-User Interface
- *User Guide for Microsoft Outlook Operating with Cisco Unified MeetingPlace Express Release 1.2* at the following URL:
http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html
- Online help found in the Microsoft Outlook plug-in application that is used to schedule Cisco Unified MeetingPlace Express meetings
- Help screens on your Cisco Unified IP Phone

Conventions

The following conventions are used in this guide:

Convention	Description
bold	Commands that you must enter exactly as shown.
<i>italic</i>	Arguments for which you supply values.
[]	Elements that are optional.
string	A set of characters that you enter. Do not use quotation marks around the string or the string will include the quotation marks.
screen	Information that appears on the screen.
^	Control key—for example, ^D means press the Control and D keys simultaneously.
< >	Nonprinting characters, such as passwords.



Tip

This action saves time and is useful.



Note

Contains important information.



Caution

Be careful. This action can result in equipment damage or loss of data.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the magazine for Cisco networking professionals. Each quarter, *Packet* delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *Packet* magazine at this URL:
<http://www.cisco.com/packet>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtunlcd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Troubleshooting Access Issues for the Cisco Unified MeetingPlace Express System

This chapter contains the following topics:

- [Recovering the Password for the root User Account, page 1-1](#)
- [Recovering the Password for the mpadmin Account, page 1-2](#)
- [Recovering the System Administrator Password Used in the End-User Interface and the Administration Console, page 1-3](#)
- [Accessing the System after Uploading the Wrong SSL Certificate or Key, page 1-4](#)
- [Troubleshooting a Failed LDAP Log On Attempt, page 1-5](#)

After reviewing this chapter, if you still have problems with Cisco Unified MeetingPlace Express, contact Cisco TAC. See the *“Obtaining Technical Assistance”* section on page vi for information on contacting Cisco TAC.

Recovering the Password for the root User Account

If you forget the password that you created for the root user account while installing the Cisco Unified MeetingPlace Express system, follow these steps to reset it:

Procedure

- Step 1** Reboot your server.
- Step 2** During the reboot, there is a period when you have only three seconds to choose to update the server configuration so that you can reset the root password. When you see a screen with the word GRUB at the top and a text box with Cisco Unified Communications in it, quickly press the spacebar.



Caution You only have three seconds to press the spacebar once the system displays this screen.



Note Nowhere on this screen does it say anything about pressing the spacebar to reset the root password.

Step 3 The system displays three options. Use the up and down arrow keys to highlight the third entry. It starts with “kernel.”

Step 4 Press **e** to edit the entry.

Step 5 At the end of the entry, enter a space and then **single**.



Note You must type a space before you type **single**.

Step 6 Press **Enter** to return the previous screen. The third entry should have the word **single** at the end.

Step 7 Press **b** to continue rebooting the server.

Step 8 At the prompt, enter **/root/.security/unimmunize.sh**.

Step 9 At the prompt, enter **passwd root**. This tells the server to set a new password for the user called root.

Step 10 At the New password: prompt, enter a new password. For security purposes, the password is displayed as a series of asterisks.



Note You may see a message that the password you entered is bad. Ignore this message.

Step 11 At the Retype new password: prompt, re-enter the same password again.

Step 12 At the prompt, enter **/root/.security/immunize.sh**.

Step 13 At the prompt, enter **reboot**. This reboots the server.

The Cisco Unified MeetingPlace Express operating system login page is displayed.

Step 14 At the username prompt, enter **root**.

Step 15 At the password prompt, enter the new password that you created in [Step 9](#).

The system should display the Cisco Unified MeetingPlace Express operating system desktop.

Recovering the Password for the mpadmin Account



Note Follow this same procedure to *change* the mpadmin account password, too.

If you forget the password that you created for the mpadmin account while installing the Cisco Unified MeetingPlace Express system, follow these steps to reset it:

Procedure

Step 1 Log in to the Cisco Unified MeetingPlace Express operating system as the **root** user.

Step 2 At the password prompt, enter the root password. (If you have forgotten the root password, first follow the steps in the [“Recovering the Password for the root User Account”](#) section on page 1-1.)

The Cisco Unified MeetingPlace Express operating system desktop appears.

Step 3 Right-click on the desktop.

Step 4 From the menu, select **New Terminal**. This brings up a terminal session.

- Step 5** At the prompt, enter `/root/.security/unimmunize.sh`.
- Step 6** At the prompt, enter `passwd mpxadmin`. This tells the server to set a new password for the user called mpxadmin.
- Step 7** At the New password prompt, enter a new password. For security purposes, the password is displayed as a series of asterisks.



Note You may see a message that the password you entered is bad. Ignore this message.

- Step 8** At the Retype new password prompt, re-enter the same password again.
- Step 9** At the prompt, enter `/root/.security/immunize.sh`.
- Step 10** On the desktop, click **RedHat > Network Services**.
- Step 11** Click **Log out**.
-

Recovering the System Administrator Password Used in the End-User Interface and the Administration Console

If you forget the password that you created for the system administrator account, which is used in the End-User Interface and Administration Center, follow these steps to reset it:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
- Step 2** At the password prompt, enter the mpxadmin password. (If you have forgotten the mpxadmin password, first follow the steps in the [“Recovering the Password for the mpxadmin Account”](#) section on page 1-2.)
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
- Step 5** At the prompt, enter `userutil -p admin <newpassword>`, where **newpassword** is the new password. This tells the server to set a new password for the End-User Interface and Administration Center user called admin.
- Step 6** On the desktop, click **RedHat > Network Services**.
- Step 7** Click **Log out**.
-

Accessing the System after Uploading the Wrong SSL Certificate or Key

To have Secure Socket Layer (SSL) work with the Cisco Unified MeetingPlace Express application, you must upload SSL certificates and enable SSL. See the *Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2* for information about doing this.



Note

The SSL certificate that you upload must be in the PEM format. If your SSL certificate is in the DER format, convert it to the PEM format and upload it again. Use this CLI command to convert a certificate from DER to PEM:

```
openssl -in <file1.crt> -inform DER -out <file2.crt>
```

where *file1.crt* is the name of the DER file and *file2.crt* is the name of the PEM file.

However, if you enter the wrong certificate or private key name and enable SSL, you cannot access the Cisco Unified MeetingPlace Express application and you are locked out.

Follow these steps to access the application:

Procedure

- Step 1** Open a web browser and navigate to <http://<localhostname>:8080>, where **localhostname** is your local hostname.
The Cisco Unified MeetingPlace Express application opens.
- Step 2** Log in to Cisco Unified MeetingPlace Express.
- Step 3** At the top of the page, click **Administration**.
- Step 4** On the left side of the page:
 - a. Click **Certificate Management**.
 - b. Click **Disable SSL**.
- Step 5** Disable SSL by clicking **Disable SSL**.
- Step 6** Restart the Cisco Unified MeetingPlace Express system by clicking **Restart Now**.
This updates the web conferencing configuration files and after the system restarts you should be able to correctly access the Cisco Unified MeetingPlace Express application.
Open a web browser and navigate to <http://<localhostname>>, where **localhostname** is your local hostname.
- Step 7** Log in to Cisco Unified MeetingPlace Express.
- Step 8** At the top of the page, click **Administration**.
- Step 9** On the left side of the page:
 - a. Click **Certificate Management**.
 - b. Click **Enable SSL**.
- Step 10** Enter the correct certificate or private key names.
- Step 11** Click **Upload Certificates**.

- Step 12** The system displays a dialog box stating that this will restart the server and to only proceed if you are sure. Click **OK** to upload the certificates, update the configuration, and restart the server.
-

If your system still does not enable SSL, the system may have overwritten the private keys that were created on the system during the initial Certificate Signing Request (CSR) generation. (This can happen if you generated new CSRs.) In this situation, the recovery steps are as follows:

Procedure

- Step 1** Log in to Cisco Unified MeetingPlace Express.
- Step 2** At the top of the page, click **Administration**.
- Step 3** On the left side of the page:
- Click **Certificate Management**.
 - Click **Generate CSRs**.
- Step 4** Enter information in the fields.
- Step 5** Click **Generate CSRs**.
- The system generates new private keys and stores them in the /usr/local/enrollment directory.
- Step 6** Send the new CSRs to the CA so that they can reissue the SSL certificates.
- Step 7** After you receive the SSL certificates from the CA, go to the Enable SSL page and upload them.
-

Troubleshooting a Failed LDAP Log On Attempt

There are certain conditions in which users may have trouble logging in to Cisco Unified MeetingPlace Express:

- If a single user is having an issue and if that user is using Cisco Unified CallManager LDAP integration and if the user cannot log in to the Cisco Unified CallManager user page, reset the password for that user in Cisco Unified CallManager. If the user still cannot log in, follow the steps in the procedure below.
- If a single user is having an issue and is using a third-party LDAP integration (such as Active Directory) and if the user cannot log in to the LDAP domain, reset the password for that user in the third-party LDAP integration. If the user still cannot log in, follow the steps in the procedure below.
- If all users are affected, check the LDAP configuration settings on the Cisco Unified MeetingPlace Express Usage Configuration page (**Administration > System Configuration > Usage Configuration**). Ensure the following:
 - The value in the LDAP URL field is correct and contains no empty spaces.



Tip To ensure that there are no empty spaces, delete the current entry and enter the LDAP value again.

- The entries for the Directory username and Password fields are correct. See the *Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2* for information about allowable values for each field.

Restart the Cisco Unified MeetingPlace Express server if you made any changes. If this does not correct the problem, follow the steps in the procedure below.

Procedure

Step 1 Log in to Cisco Unified MeetingPlace Express as the user called admin.



Note For information on logging in to Cisco Unified MeetingPlace Express, see the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2*.

Step 2 Capture the system information by following these steps:

- In Cisco Unified MeetingPlace Express click **Administration** in the top menu bar.
- On the left, click **Services**, then **Logs**, then **View System Information Capture**.
- Enter the information into the form. In the Approximate event time field, enter a time that is about the time when you tried to log in using the LDAP mechanism.
- Enter 10 in the Log capture window field.
- Click **View Logs**.
- At the pop-up message, click **OK**.
- Save the file created by clicking **Export to File**.

Step 3 Forward the saved file to Cisco TAC.

If you are using Cisco Unified CallManager, remember the following:

- Ensure that you can log in to the Cisco Unified CallManager Data Connection Directory.
For example, in Cisco Unified CallManager go to **Programs > DC Directory Administration**. Log in as the Directory Manager with the password that you specified in the Password field on the Cisco Unified MeetingPlace Express Usage Configuration page (**Administration > System Configuration > Usage Configuration**).
- Ensure that the first time a user logs in to Cisco Unified MeetingPlace Express, he uses the End-User Interface.



Note When a user logs in for the first time, Cisco Unified MeetingPlace Express creates a profile for that user “on the fly.” A successful login (and the message *Welcome “User”*) means that the user’s profile was successfully created. If the user attempts to log in for the first time using the Telephone User Interface (TUI), the system will not create a profile.

- Ensure that the user profile is not locked in Cisco Unified CallManager. (User profiles become locked after too many failed attempts to log in.)
- Check the Cisco Unified MeetingPlace Express log in the following location:
`/opt/cisco/meetingplace_express/tomcat/current/logs/bounty.out`



Backing Up, Archiving, and Restoring Data in Cisco Unified MeetingPlace Express

This chapter contains the following troubleshooting topics:

- [Backing Up Data, page 2-1](#)
- [Archiving Data, page 2-2](#)
- [Restoring Data, page 2-2](#)

After reviewing this chapter, if you still have problems with Cisco Unified MeetingPlace Express, contact Cisco TAC. See the *“Obtaining Technical Assistance” section on page vi* for information on contacting Cisco TAC.

Backing Up Data

You can use the Cisco Unified MeetingPlace Express Administration Center to configure the system to automatically back up data.

If you choose to disable the automatic back up feature, you can still manually back up data. However, if you disable the automatic backup, be sure to only run one backup at a time.

To manually back up data, follow these steps:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
 - Step 2** At the password prompt, enter the mpxadmin password.
The Cisco Unified MeetingPlace Express operating system desktop appears.
 - Step 3** Right-click on the desktop.
 - Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
 - Step 5** Manually back up the data by entering the following:
sudo \$MP_DATABASE/db-maintenance/backup.sh
 - Step 6** On the desktop, click **RedHat > Network Services**.
 - Step 7** Click **Log out**.
-

Archiving Data

You can use the Cisco Unified MeetingPlace Express Administration Center to configure the system to automatically archive data. However, if you want to manually archive data, follow these steps:

Procedure

-
- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
 - Step 2** At the password prompt, enter the mpxadmin password.
The Cisco Unified MeetingPlace Express operating system desktop appears.
 - Step 3** Right-click on the desktop.
 - Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
 - Step 5** Manually archive the data by entering the following:

```
sudo $MP_DATABASE/db-maintenance/archive.sh
```



Note The archive.sh script uses remote log-in credentials that are defined in the \$MP_DATABASE/db-maintenance/settings.config file. You can set these credentials through the Cisco Unified MeetingPlace Express Administration Center.

- Step 6** On the desktop, click **RedHat > Network Services**.
 - Step 7** Click **Log out**.
-

Restoring Data

Restoring data recreates the database server data from backed-up storage spaces and logical log files. You may need to restore your data if you need to replace a failed disk that contains database server data, if there is a logic error in a program that has corrupted the database, if you need to move your database server data to a new computer, or if a user accidentally corrupts or destroys data.

To restore data up to the time of the failure, you must have at least one L0 backup. The restore is done using the Informix command called **ontape**. Cisco Unified MeetingPlace Express provides a script called restore.sh that guides you through the restore process. The script is in the \$MP_DATABASE/db-maintenance directory.

Backups have several levels (L0, L1, and L2). To restore the data, you must have the backup files in the correct order. For example, if you have the correct L0 and L2 backup files, but not the appropriate L1 backup file, you cannot restore the data. This requires extra caution if you manually back up files on a local disk or in the archiving location.



Caution

You can only restore a database that is from the same version of the Cisco Unified MeetingPlace Express product. You cannot restore a database from a previous version.

The names of the databases that you are restoring from and restoring to must be the same.

Follow these steps to restore data from a backup file:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
- Step 2** At the password prompt, enter the mpxadmin password.
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
- Step 5** Shut down the Cisco Unified MeetingPlace Express application by entering the following:
mpx_sys stop
- Step 6** Restore the data by entering the following:
sudo \$MP_DATABASE/db-maintenance/restore.sh
- Step 7** On the desktop, click **RedHat > Network Services**.
- Step 8** Click **Log out**.
-



Common Telephone Issues in Cisco Unified MeetingPlace Express

This chapter contains the following topics:

- [Tips for Failed Calls, page 3-1](#)
- [Undetected Key Presses, page 3-2](#)
- [Failed Incoming Calls, page 3-3](#)
- [Dropped Calls, page 3-3](#)
- [Dead Air During Calls, page 3-4](#)
- [Dropped Packets, page 3-4](#)
- [Unable to Call Out, page 3-5](#)

After reviewing this chapter, if you still have problems with Cisco Unified MeetingPlace Express, contact Cisco TAC. See the *“Obtaining Technical Assistance”* section on page vi for information on contacting Cisco TAC.

Tips for Failed Calls

The following tips should always be used when troubleshooting failed calls:

- Look for network congestion at the time of the call. Network congestion information can be found via router and switch statistics.
- Ensure that the Cisco Unified MeetingPlace Express system is set to full-duplex with 100 Mbps network speed.
- Ensure that the local switch port for the Cisco Unified MeetingPlace Express system has the same auto-negotiation setting as the Cisco Unified MeetingPlace Express system. You can run the **mii-tool** command from the CLI to see the current link setting.
- If Cisco Unified MeetingPlace Express and the local switch (or router) are configured correctly, make sure that the network on the other side of the switch or router is also set to 100 Mbps, full duplex.
- Ensure that the Cisco Unified MeetingPlace Express system is not connected to a multiple-device Ethernet bus. The system works best if micro-segmented to use a single switch port rather than share a bus with other devices. Sharing a bus can cause excessive collisions which reduce bandwidth and cause unpredictable bandwidth availability.

- If there is still congestion, you may have to take standard congestion reduction measures such as these:
 - Reduce traffic in the local LAN by adding more switches and distributing the network devices between them.
 - Reduce the number of devices on the local LAN (and thus the traffic) by adding more routers to create more (but smaller) LANs. There might also be unused ports on the local router in which case more routers are not needed.
 - Change network device settings to reduce unnecessary traffic such as adding Access Control Lists (ACLs) to the local router to filter out irrelevant traffic.
- Get a trace of network traffic. This trace should be taken as close to the eth0 port as possible.
- Some phones provide network error statistics about how many bad frames have been received. See if the particular phone has these statistics. If so, see if the phone has registered the reception of a large number of bad frames.
- Verify the configuration of the device that routes calls to Cisco Unified MeetingPlace Express.
- Check for any firewalls between the phone and Cisco Unified MeetingPlace Express that may prevent calls.

Undetected Key Presses

If it appears that the Cisco Unified MeetingPlace Express system is not detecting you when you press the keys on your phone, try these steps:

Procedure

-
- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the root user.
- Step 2** At the password prompt, enter the root password.
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
- Step 5** At the CLI, enter the following:
eventlog -b<mmddhhmm> -e<mmddhhmm>
For the start time (the -b value), enter a time shortly before the call failed. For the stop time (the -e value), enter a time shortly after the call failed.
- Step 6** Check the DID/DNIS and input events to determine which port is yours.
- Step 7** Look later in the trace to see if DTMFs sent from your phone were being detected. If they are not detected, then check the following:
- Verify that the telephony network is using RFC 2833 digits or out-of-band digits. (The Cisco Unified MeetingPlace Express system does not support in-band digits.)
 - Network congestion might be preventing the RFC 2833 digits or out-of-band digits from reaching the system.

- Check if G.729 coders are being used somewhere in your network, instead of G.711. G.729 will seriously corrupt in-band digits (DTMF) causing these digits to either be lost or changed. If this is happening and RFC 2833 is *not* a good choice, consider converting to a pure G.711 network.
-

Failed Incoming Calls

If you are not able to receive incoming calls, do the following:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the root user.
- Step 2** At the password prompt, enter the root password.
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.
- Step 5** At the CLI, enter the following:
eventlog -b<mmddhhmm> -e<mmddhhmm>
For the start time (the -b value), enter a time shortly before the call failed. For the stop time (the -e value), enter a time shortly after the call failed.
- Step 6** Determine if the Cisco Unified MeetingPlace Express system registered the call signaling packets.
- If the system registered the call, look for a reason in the trace log why the call was disconnected. Enter one of these commands:
eventlog -b<mmddhhmm> -e<mmddhhmm> -v
eventlog -b<mmddhhmm> -e<mmddhhmm> -G -v
 - If the system did not register the call in the trace log, the problem might be a configuration problem on the device that routes calls to Cisco Unified MeetingPlace Express. Also, check if any firewalls may be preventing the call from reaching the system.
-

Dropped Calls

If calls are connected to the system, but then disconnect during the call, do the following:

Procedure

- Step 1** Log in to the Cisco Unified MeetingPlace Express operating system as the root user.
- Step 2** At the password prompt, enter the root password.
The Cisco Unified MeetingPlace Express operating system desktop appears.
- Step 3** Right-click on the desktop.
- Step 4** From the menu, select **New Terminal**. This brings up a terminal session.

- Step 5** At the CLI, enter the following:
eventlog -b<mmddhhmm> -e<mmddhhmm>
- For the start time (the -b value), enter a time shortly before the call failed. For the stop time (the -e value), enter a time shortly after the call failed.
- Step 6** Check for a “far end disconnect event.” If you see this, the disconnect may have been initiated outside of the Cisco Unified MeetingPlace Express system. Check for errors on the devices between the phone and the Cisco Unified MeetingPlace Express system.
- Step 7** If you do not see a “far end disconnect event,” the Cisco Unified MeetingPlace Express system hung up on you first. Review the trace log to try to determine why the system hung up on you.
- Step 8** If your system uses Cisco Unified CallManager contact the Cisco Unified CallManager network administrator to get a call session trace indicating why Cisco Unified CallManager sent the disconnect event to you.
-

Dead Air During Calls

If you think that your call has been disconnected, but your phone still shows that the call is active, follow these steps:

Procedure

- Step 1** If you are in a meeting, enter **#21** to hear a roll call of all meeting participants.
 Do you hear anything?
- If yes, you have at least one-way audio (that is, you can hear but not speak).
 - If you do not hear anything, either there is no audio either way or Cisco Unified MeetingPlace Express cannot detect your DTMF keypresses.
- Step 2** Provide this information to your network administrator and try to get a call session trace from Cisco Unified CallManager.
-

Dropped Packets

If you determine that packets are being dropped (as determined by RTCP statistics) or delivered with errors and then dropped at the endpoints, consider changing the following call configuration parameters:

Procedure

- Step 1** Log in to Cisco Unified MeetingPlace Express.
- Step 2** At the top of the page, click **Administration**.
- Step 3** On the left side of the page:
- a. Click **System Configuration**.
 - b. Click **Call Configuration**.

c. Click **Audio Parameters**.

Step 4 In the Default G.711 packet size (milliseconds) field, enter **10**.

A smaller packet size reduces the damaging effect of a lost packet. However, network traffic increases slightly.

Step 5 Set the Voice activity detect field to **yes**.

This reduces outgoing packets to callers. The Cisco Unified MeetingPlace Express system only transmits packets if someone is actively speaking during a meeting. However, there might be a slight delay when someone starts speaking causing part of their initial syllable to not be heard.

Step 6 Determine how to configure the phones in your organization to use Voice Activity Detect (VAD). This way, the phones only send packets to the Cisco Unified MeetingPlace Express system when the phone detects sound on your handset or headset.

Step 7 Set the Maximum jitter buffer (milliseconds) field to **250**.

This is the maximum value allowed. This higher value introduces more delays into conversations, but also reduces packet loss due to sudden surges in traffic.

Step 8 To maximize bandwidth, have the network administrator check that the your Cisco Unified MeetingPlace Express system and the local switch that your system connects to are both running in 100 Mbps full duplex mode.

Unable to Call Out

If users are unable to make calls out of the system, do the following:

- Ensure that the H.323 ID field is not blank. To check this, go to the H.323 Call Configuration page of the Administration Center.

If an individual user is unable to make calls out of the system, do the following:

- If the user is a profiled user, go to the Edit User Profiles page and ensure that the **Can call out of meetings** field is set to **Yes**.
- If the user is a guest user, do both of the following:
 - Go to the Usage Configuration page and ensure that the **Allow guest outdials** field is set to **Yes**.
 - Go to the Edit User Profiles page and ensure that the **Can call out of meetings** field is set to **Yes** for the user profile called guest.



Exception Codes and Module Numbers Used in Cisco Unified MeetingPlace Express

This chapter contains information about the exception codes used in the Cisco Unified MeetingPlace Express system. After reviewing this chapter, if you still have problems with Cisco Unified MeetingPlace Express, contact Cisco TAC. See the *“Obtaining Technical Assistance” section on page vi* for information on contacting Cisco TAC.

Exception Codes

The Cisco Unified MeetingPlace Express system generates exception codes whenever there is an internal problem. There are many exception codes and they are not all documented here. Only the most meaningful codes and those that you can possibly fix are included.

To find these error codes, run the **errorlog** CLI command.

[Table 4-1](#) contains the most frequently seen and important exception codes for the Cisco Unified MeetingPlace Express system.



Note

Some exception codes are listed as a decimal number and others as a hexadecimal number. For clarification, both code numbers are listed.

Table 4-1 Important Exception Codes in Cisco Unified MeetingPlace Express

Code (Dec)	Code (Hex)	Severity	Display Text	Comments
131157	0x20055	MAJOR	Time has been set backwards. Some resource reservations may be lost.	The system clock has been set back to at least the previous month since the last time the Cisco Unified MeetingPlace Express application was running. This can result in loss of some resource reservation records. Recommended Action: Verify the system clock. Always shut down the Cisco Unified MeetingPlace Express application before changing the clock.
131192	0x20078	MAJOR	The CS is behind ## seconds. Conf ##, Next Event ##, Time ##	The conference management software has fallen behind processing conference life cycle events. This can indicate the system is overloaded. It can be a normal result of a system being down for a while. Repeated alarms about a failure to catch up may indicate a software defect. Recommended Action: No action required.
131198	0x2007E	INFO	No ports left to extend meeting. Erc ##, Now ##, Length ##, Ports ##	The Cisco Unified MeetingPlace Express system was unable to extend a meeting due to lack of available voice ports. Recommended Action: No action required.
196686	0x3004E	MINOR	Too many conference events. Next event = ##, Conf = ##, Max events = ##	Probably indicates too many people entering or leaving a meeting at the same time, overloading the ability of the Cisco Unified MeetingPlace Express system to queue up entry or exit announcements. Recommended Action: No action required.

Table 4-1 Important Exception Codes in Cisco Unified MeetingPlace Express (continued)

Code (Dec)	Code (Hex)	Severity	Display Text	Comments
196848	0x300F0	MINOR	Allocation of access ports to units has been fixed. Thank you!	A “too many access ports” condition (see error message 0x300F1) has been resolved. Recommended Action: No action required.
196849	0x300F1	MINOR	Too many access ports compared to licenses ##.	The configured number of voice ports exceeds the number of valid licenses, where ## is the configured value. This may be caused by the license being temporary expired. Recommended Action: No action required.
196943	0x3014F	WARN	FLEXLM: Failed to connect to license server; status = ##.	The license manager is not running, probably because no valid licenses are installed. Recommended Action: No action required.
196944	0x30150	MINOR	No conferencing licenses are installed.	The system has no valid licenses installed for either voice or web conferencing. The system defaults to six voice conferencing licenses. Recommended Action: Obtain and install licenses.
196946	0x30152	WARN	Unexpected LDAP response.	An unexpected response from the LDAP server, possibly indicating an incompatibility between systems. Recommended Action: No action required.
196950	0x30156	MINOR	Password authentication mechanism failure.	The password authentication feature is not working. Recommended Action: Check for an LDAP configuration problem or an LDAP server failure.

Table 4-1 Important Exception Codes in Cisco Unified MeetingPlace Express (continued)

Code (Dec)	Code (Hex)	Severity	Display Text	Comments
196953	0x30159	MINOR	Password authentication failure; may need to configure or application restart.	The password authentication feature is not working. Recommended Action: Check for an LDAP configuration problem or an LDAP server failure. Try restarting the application.
196959	0x3015F	INFO	No voice conferencing licenses are installed.	The system has a web conferencing license installed but no voice conferencing license. Recommended Action: Install voice conferencing licenses.
458788	0x70024	MAJOR	Module timed out on “are you there” query, class=##	One of the major software modules (identified by the class number) failed to respond to a query from the system integrity manager (SIM). This restarts the system. Recommended Action: Report all such occurrences to Cisco TAC for problem diagnosis.
458889	0x70089	WARN	Stopping exception log due to flooding.	The exception logging process stops logging if incoming messages exceed a certain rate. This prevents the logging mechanism from stealing critical resources when the system is overloaded. Recommended Action: No action required.
458890	0x7008A	INFO	Lost ## exception events; logging resumed.	The exception logging process dropped the indicated number of messages due to overload. Normal logging has now resumed. Recommended Action: No action required.

Table 4-1 Important Exception Codes in Cisco Unified MeetingPlace Express (continued)

Code (Dec)	Code (Hex)	Severity	Display Text	Comments
458916	0x700A4	MAJOR	System crashed: restarted by the integrity manager.	Alarm generated as the system comes back up; triggered by a flag set during a reboot initiated by the system integrity manager (SIM). Recommended Action: No action required.
1572903	0x180027	INFO	CPGS: Too many conference participants; can't create voice file.	The cumulative number of guest participants in a meeting has exceeded the system's ability to store name recordings for that meeting. The user name is not being recorded. This normally happens only during stress testing. Recommended Action: No action required.
1572914	0x180032	MINOR	CPGS: No space available for recording	Start of recording failed due to lack of disk space. Recommended Action: Purge old recordings.
2097190	0x200026	WARN	NMPAgent received late response (class=##, code=##)	The telephony or scheduling part of the system is running very slow, possibly due to overload. Recommended Action: No action required.
2162708	0x210014	MINOR	POC: Invalid email address for scheduler (##)	The meeting scheduler does not have a valid e-mail address; cannot send e-mail to that user. ## is the unique user ID of the scheduler. Recommended Action: No action required.
2162710	0x210016	WARN	POC: E-mail not sent. Client is not authenticated.	E-mail rejected by e-mail exchanger due to authentication failure. Likely an SMTP configuration problem. Recommended Action: No action required.

Table 4-1 Important Exception Codes in Cisco Unified MeetingPlace Express (continued)

Code (Dec)	Code (Hex)	Severity	Display Text	Comments
2162712	0x210018	WARN	POC: E-mail not sent. SMTP servers are unavailable.	Failed to connect to an SMTP e-mail exchanger. The exchanger may be down or there may be a problem with the SMTP configuration. Recommended Action: No action required.
2162713	0x210019	WARN	POC: E-mail not sent. Address format is invalid.	A recipient's e-mail address was rejected due to an invalid format. Recommended Action: No action required.
2162714	0x21001A	WARN	POC: SMTP server failed to deliver e-mails due to unknown recipient.	The SMTP e-mail exchanger rejected a recipient's e-mail address as unknown. Recommended Action: No action required.
2260993	0x228001	MINOR	Connection to web conferencing service restored.	Successfully reconnected to the web conferencing server. Recommended Action: No action required.
2260994	0x228002	MINOR	Error connecting to web conferencing service. Trying again...	Trying to reconnect to the web conferencing server. Recommended Action: None needed as long as the "Connection to web conferencing service restored" message is logged subsequent to this message. If that message is <i>not</i> logged, then the system may need to be restarted or serviced.
2260995	0x228003	MINOR	Lost connection to web conferencing service. Trying again...	Trying to reconnect to the web conferencing server. Recommended Action: None needed as long as the "Connection to web conferencing service restored" message is logged subsequent to this message. If that message is <i>not</i> logged, then the system may need to be restarted or serviced.

Module Numbers

Some Cisco Unified MeetingPlace Express error messages refer to a module number but do not give the name of the corresponding system component.

The following is an example of an error message:

**11/11 15:13:37.13 MAJ 0x70041 0/2, "siupdown.cc", 265 (0x8, 0, 0, 0)
Restarting due to software module failure, module = 8**

In the second line of this example, it says module = 8, which, based on [Table 4-2](#), indicates that the error was caused by the Telephone User Interface.

[Table 4-2](#) converts the module numbers to system component names.

Table 4-2 *Module Numbers and Names*

Internal Error Number	System Component	Module Number	Description
0	IMC_CLASS_NULL	0	
1024	IMC_CLASS_COMMON	1	Common functions
2048	IMC_CLASS_SIM	2	System Integrity Manager (SIM)
3072	IMC_CLASS_CP	3	Call processing
4096	IMC_CLASS_SM	4	Switch manager
5120	IMC_CLASS_CS	5	Conference scheduler = ERC_BAD
6144	IMC_CLASS_WS	6	Workstation server
7168	IMC_CLASS_EXC	7	Exception handler (in SIM)
8192	IMC_CLASS_VUI	8	Telephone user interface
9216	IMC_CLASS_DB	9	The database server
10240	IMC_CLASS_VUI_TESTER	10	TUI tester program
11264	IMC_CLASS_TRACE	11	SIM trace server
12288	IMC_CLASS_WF	12	Workstation front end
13312	IMC_CLASS_UTIL	13	Any command line utility
14336	IMC_CLASS_LSH	14	Shell facility
15360	IMC_CLASS_DBQ	15	Database query server
16384	IMC_CLASS_EMAIL_MSG	16	Class to support an error range
17408	IMC_CLASS_SNMPD	17	Class to support SNMP daemon control
18432	IMC_CLASS_PO	18	Post office server
19456	IMC_CLASS_PO_TESTER	19	Post office server tester program
20480	IMC_CLASS_SIM_MU	20	Multi-unit SIM session control
21504	IMC_CLASS_FAXGW	21	Fax gateway
22528	IMC_CLASS_WEBGW	22	Web publisher (overlaps with pegs)
22528	IMC_CLASS_PEGS	22	Peg server (part of SIM)
23552	IMC_CLASS_SDBS	23	Shadow database server

Table 4-2 *Module Numbers and Names (continued)*

Internal Error Number	System Component	Module Number	Description
24576	IMC_CLASS_SDBS_TESTER	24	Shadow database server tester program
25600	IMC_CLASS_GWSIMGR	25	
26624	IMC_CLASS_GWSIMAGENT	26	
27648	IMC_CLASS_STREAMGW	27	Streaming gateway
28672	IMC_CLASS_CCA	28	Call control agent
29696	IMC_CLASS_MPDIRSVC	29	Directory services
30720	IMC_CLASS_MERGED	30	PCI conversion/merge daemon
31744	IMC_CLASS_GSCOPE	31	Gyroscope application
32768	IMC_CLASS_NMPAGENT	32	NMPAgent
33792	IMC_CLASS_TWATCH	33	Trigger watch
34816	IMC_CLASS_POCLIENT	34	Post office client



General Troubleshooting Tips for the Cisco Unified MeetingPlace Express System

This chapter contains the following troubleshooting topics:

- [Swapping Out a Disk Drive, page 5-9](#)
- [File Locations, page 5-10](#)
- [Troubleshooting a Licensing Error Problem, page 5-11](#)
- [Troubleshooting a Problem with Excessive Random E-Mails Being Sent, page 5-11](#)

After reviewing this chapter, if you still have problems with Cisco Unified MeetingPlace Express, contact Cisco TAC. See the *“Obtaining Technical Assistance”* section on page vi for information on contacting Cisco TAC.

Swapping Out a Disk Drive

This section describes how to swap out a hard-disk drive on your Cisco MCS server. Each Cisco MCS server has multiple hard-disk drives so it is possible to continue using the Cisco Unified MeetingPlace Express system if a hard-disk drive fails. However, there will be no redundancy and if the system goes down, you can lose your operating system, application, and data.

Before You Begin

- Step 1** Determine the model number of your Cisco MCS server.
 - Step 2** Determine which hard-disk drive on your Cisco MCS server has failed.
 - Step 3** Order the replacement hard-disk drive. The replacement hard-disk drive must be the same model as the one it is replacing.
-

Swapping Out a Disk Drive on a Cisco MCS 7825

All versions of the Cisco MCS 7825 have front-accessible, simple-swap SATA (Serial Advanced Technology Attachment) hard-disk drives. The SATA hard-disk drives are accessible through openings in the front bezel of the server. If a hard-disk drive fails, schedule server downtime, power down the server, and replace the failed SATA drive by removing it (each drive is equipped with a front latch that positively mates the drive to the server) and replacing it with an unconfigured spare hard-disk drive.

Follow these steps to change the disk:

Procedure

-
- Step 1** Turn off the server and all peripheral devices.
 - Step 2** Disconnect the power cord and all external cables.
 - Step 3** Remove the bad hard-disk drive.
 - Step 4** Insert the new hard-disk drive.
 - Step 5** Connect the power cord and all external cables.
 - Step 6** Turn on the power.
 - Step 7** Reinstall the Cisco Unified MeetingPlace Express operating system and restore the application and your data from a backup.
-

Swapping Out a Disk Drive on a Cisco MCS 7835 or Cisco MCS 7845

All versions of the Cisco MCS 7835 and the Cisco MCS 7845 support up to six Small Computer System Interface (SCSI) hot-plug hard drives (or five hot-plug hard drives and one hot-plug tape drive) that are configured using RAID 1. These are hot-swappable SCSI drives, so you can change them without powering down the server.

Follow these steps to change a hard-disk drive if it fails:

Procedure

-
- Step 1** Remove the bad hard-disk drive.



Note You do not need to turn off the power on your system.

- Step 2** Insert the new hard-disk drive.
-

The system automatically synchronizes the new disk with no interruption.

File Locations

System administrators use several files. [Table 5-1](#) lists the locations of several common files.

Table 5-1 File Locations

Location	Description
/lat/bin	Contains most of the executable files
/var/mp	Contains most of the stderr and stdout files
/opt/cisco/meetingplace_express/application/logs	Contains most of the logs
/opt/cisco/meetingplace_express/application/versions	Contains a directory for each version installed
/opt/cisco/meetingplace_express/uninstaller	Contains the uninstall script
/opt/cisco/meetingplace_express/database/db-maintenance	Contains the backup, archive, and restore database scripts

Troubleshooting a Licensing Error Problem

Problem I'm trying to install a license and get an error that says "Sorry. Cannot enter the license at this time." Why?

Solution The hostname that you entered during the product installation contains more than 32 characters. Use the **net** command to change the hostname of the system so that it contains 32 characters or less. See the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2* for information about the **net** command.

Problem I am using Cisco Unified CallManager Release 5.x and whenever I try to subscribe to the Cisco Unified MeetingPlace Express service for the Cisco Unified IP Phone with the correct username and PIN, the login always fails. The phone screen shows an Authentication fails message. Why?

Solution This is a known bug. The workaround is to go into the Cisco Unified CallManager administration area, navigate to the Cisco Unified MeetingPlace Express service, make no changes, and click **Update Subscriptions**.



Note This problem does not occur with Cisco Unified CallManager Release 4.x and earlier.

Troubleshooting a Problem with Excessive Random E-Mails Being Sent

Problem The Cisco Unified MeetingPlace Express system is sending out excessive e-mails and this is crashing our e-mail and voice mail system. What can I do to stop this?

Solution The e-mails are generated by the cron script. The cron daemon sends an e-mail report of all its jobs to the e-mail address that is configured in the crontab file. To disable the e-mails, manually edit the crontab file and change the line with MAILTO to read MAILTO=""

Troubleshooting a Problem with the Web Page Not Coming Up

Problem After installing the Cisco Unified MeetingPlace Express system, the home page does not appear.

Solution Make sure that you correctly set the host name values during installation. If you entered incorrect information, use the **net** command to change the values. See the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2* for complete information about how to use the **net** command.



A

- accessing the system [1-4](#)
- archiving data
 - about [2-2](#)
 - definition [2-2](#)
- auto-negotiation [3-1](#)

B

- backing up data
 - about [2-1](#)
 - definition [2-1](#)
- backups
 - L0 [2-2](#)

C

- Certificate Signing Request (CSR) [1-5](#)
- Cisco MCS 7835-H1-RC1
 - swapping disk drive [10](#)
- Cisco Unified MeetingPlace Express
 - common telephone errors [3-1](#)
 - related documentation [ii](#)
 - troubleshooting [1-1, 2-1, 4-1, 9](#)
 - accessing the system [1-4](#)
- commands
 - archive [2-2](#)
 - backup [2-1](#)
 - errorlog [4-1](#)
 - immunize [1-2](#)
 - infocap [3-2, 3-4](#)
 - mii-tool [3-1](#)

- ontape [2-2](#)
- passwd [1-3](#)
- restore [2-3](#)
- unimmunize [1-3](#)
- userutil [1-3](#)

Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2

- location online [ii](#)

D

- disk drives
 - swapping [9](#)
- duplex
 - troubleshooting [3-1](#)

G

- G.711 [3-3](#)
- G.729 [3-3](#)
- Guide to Cisco Unified Conferencing Documentation and Support
 - location online [ii](#)

I

- Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2
 - location online [ii](#)

J

- jitter buffer [3-5](#)

L

L0 backup [2-2](#)

M

module numbers [4-7](#)

P

packet size [3-5](#)

passwords

changing for mpadmin user [1-2](#)

for mpadmin user [1-2](#)

for root user [1-1](#)

for system administrator [1-3](#)

recovering [1-1](#)

private keys

uploading [1-4](#)

R

reference documentation

Configuration and Maintenance Guide for Cisco Unified MeetingPlace Express Release 1.2 [ii](#)

Guide to Cisco Unified Conferencing Documentation and Support [ii](#)

Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 1.2 [ii](#)

User Guide for Cisco Unified MeetingPlace Express Release 1.2 [ii](#)

User Guide for Microsoft Outlook Operating with Cisco Unified MeetingPlace Express Release 1.2 [ii](#)

restoring data

about [2-2](#)

definition [2-2](#)

RFC 2833 [3-2](#)

S

SATA hard-disk drives [10](#)

speed

troubleshooting [3-1](#)

SSL certificates

accessing the system [1-4](#)

troubleshooting [1-4](#)

system administrator

recovering lost password [1-3](#)

system clock exception code [4-2](#)

T

trace log [3-4](#)

troubleshooting

dead air during calls [3-4](#)

dropped calls [3-3](#)

dropped packets [3-4](#)

failed calls [3-1](#)

failed incoming calls [3-3](#)

LDAP configuration [4-4](#)

swapping out disk drives [9](#)

undetected key presses [3-2](#)

U

User Guide for Cisco Unified MeetingPlace Express Release 1.2

location online [ii](#)

User Guide for Microsoft Outlook Operating with Cisco Unified MeetingPlace Express Release 1.2

location online [ii](#)

V

VAD [3-5](#)

voice activity detect

see VAD